EXHIBIT 1-A

Is Your Vote Secure in Michigan? Cybersecurity Expert Alex Halderman is Cautiously Optimistic

The notoriously pessimistic University of Michigan computer security expert says there's a lot of positive things happening in the state

By **Steve Friess** and **Illustration by Jason Raisch** - September 4, 2020

Alex Halderman

For the first time in the eight years I've been writing about him, Alex Halderman has something positive to say about an election system. He's usually a cheerful person, until the conversation turns to cyberthreats to democracy, and then he becomes the fellow who three years ago sat before the U.S. Senate's Select Committee on Intelligence, to darkly declare, "I know America's voting machines are vulnerable because my colleagues and I have hacked them —

Huh? Huh!

"The state has so far resisted the urge to allow remote voting by email," Halderman, 39, says via phone from his parents' home in suburban Pennsylvania, where he and his wife are hunkered down amid the pandemic. "It continues to offer paper ballots, and, unlike states that have implemented ballot-marking devices for every voter, the vast majority of ballots in Michigan are filled out by hand. Michigan added online absentee ballot applications and voter registration — which does require careful security practice to implement well — but unlike online voting, that's something we now have reasonably secure."

Also, Michigan is likely to conduct a special kind of post-election review known as a risk-limiting audit, or RLA, of the 2020 presidential race that is designed to detect any major discrepancy between the paper ballots and the machine-counted tally that could suggest widespread vote-changing fraud. Halderman and others have been pushing states to do this for years, and now, finally, Michigan is one of eight states with plans for some form of RLAs, according to the National Conference of State Legislatures. Four other states, including Ohio, have made RLAs optional.

Perhaps it shouldn't be so surprising that Halderman is *relatively* pleased — he does have what he calls "caveats" that we'll get to — with where Michigan is right now. After all, Secretary of State Jocelyn Benson appointed him in March 2019 as co-chair of her Election Security Commission, an 18-person panel that includes elections officials and other computer scientists. The group was due to issue a report by the end of the summer; it was delayed from earlier this year by the coronavirus crisis, but the core recommendations include the RLA, Benson spokesman Jake Rollow says.

Ingham County Clerk Barb Byrum, a member of the commission, says the meetings were a chance for cybersecurity experts like Halderman, who often rail to the media about problems they observe, to speak directly with elections officials who actually have responsibility for securing the vote. Often, she says, Halderman and others like him will draw public attention to security lapses based on lab conditions in which they have unlimited access to voting machines or tabulators, but such access is quite rare. That may have helped Halderman come to a more accurate understanding of the risks, she says.

"We are able to speak to each other, and a lot of the preconceived thoughts about elections and how secure or insecure we were or will be were debunked," she says. "Rather than throwing stones, we were speaking to each other. That is the first step to making our elections more secure."

Motivated by 2000

In computer science circles, Halderman was a rock star long before he went to Capitol Hill to scare the bejesus out of everybody about the fragility of American democracy. As a Princeton graduate student, he and his mentor, professor Ed Felten, showed how easy it was to defeat Sony BMG's attempts to prevent piracy.

man in a trench coat who handed him a large leather briefcase containing the contraband voting machine. A few months later, the team posted a video online, showing the machine being hacked in a mock election in which Benedict Arnold wins the presidency despite voters clearly choosing George Washington.

That sort of cheeky antic became a signature feature of Halderman's efforts to alert the public to technological insecurities. In 2010, most notably, the District of Columbia was planning to allow residents to vote via the internet in municipal elections. Online voting is, to Halderman, a particularly terrible idea and one he has worked against by exposing security flaws in systems used in Australia, Estonia, and Norway.

To demonstrate and test the district's system to the public, the city held a mock election a few weeks before Election Day. Halderman — then in his second year at U-M — saw this as "a fantastic opportunity to test out attacks in a live system but not an actual election." His team easily broke in, altering votes without detection. In fact, the only reason anyone noticed the breach was the music on the "thank you for voting" page: His students had set the system to play "The Victors." D.C. officials ditched the online voting idea and never returned to it.

This June, Halderman was at it again as Delaware attempted to allow voters to download ballots, mark them electronically, and then email them in for the state's July 7 primary. Ballot-marking software, which is used widely to help people with physical disabilities fill out their ballots at home, can be manipulated by software to change votes as the ballots are transmitted via the internet to their destination. That problem is usually prevented by the voter printing out the ballot and mailing it in, but Delaware wanted to let people skip that step.

Mock the vote: Alex Halderman holds an experimental election at the University of Michigan in 2018 to show how vulnerable voting machines are to hacking. // Photograph by Levi Hutmacher/Michigan Engineering, Communications & Marketing

After Halderman co-wrote a June 7 paper describing the system's vulnerabilities, Delaware hit pause on the email option. "My team and I did the security analysis and, basically, there's no magic to it," Halderman says. "It's just another online portal for uploading or sending PDF files. That means that there's no way for election officials, the voter, or the company who makes the system to actually be sure that the ballot that the voters filled in is the same as what election officials receive and count."

Halderman is especially pleased with the emphasis on paper ballots in Michigan and renewed concerns about how they're managed. In 2016, he led a large group of computer scientists that urged Democrat Hillary Clinton, who declined, and then Green Party candidate Jill Stein to demand recounts of votes cast in several states to ensure that the reported outcomes — narrow wins for Donald Trump — were accurate. That led to weeks of drama that bled past Thanksgiving and included a full recount in Wisconsin and a partial one in Michigan before state courts halted it.

In Michigan, recounts in many Detroit precincts were impossible because poll workers had not stored the paper ballots and the tabulator counts properly. Since then, Rollow says, the Legislature has provided matching funds to jurisdictions seeking to replace older and more vulnerable tabulators, and Benson's office has emphasized training on how to handle elections materials after Election Day.

Also, the expected RLA is a big deal. A risk-limiting audit is a process by which a certain number of ballots are selected at random for a hand check. If the results are within a small margin of error of the results reported by the machine count, statisticians determine that the machine count is accurate and there's no evidence of widespread fraud. If the results are out of whack, more ballots are hand-counted at random until either the results do match the machine outcome or until all ballots are hand-counted. Such an audit is cheaper and faster than going directly to a full recount.

Michigan conducted its first statewide RLA — the largest ever in the U.S. — as an experiment after the presidential primaries on March 10. State officials rolled dice to decide which 669 ballots from 277 jurisdictions would be randomly sampled and found that the results "mirrored the state's official election results within 1 percentage point for the leading candidates in each primary, suggesting if an

My homeowner association in Washtenaw County held its membership meeting in the Superior Township meeting hall where, shockingly, the township's ballot tabulators sat out unprotected in the back of the room. Sensing a major security risk, I emailed Halderman, and 15 minutes later, he and his graduate students came by to snap photos. Nobody touched the machines, but Halderman says an attacker easily could have infected one of the tabulators with an undetectable vote-changing virus. What's more, when those tabulators went online to transfer the vote tallies to the county, had they been hacked, a virus could have entered the countywide system and then the state system, he says.

"This equipment is supposed to be stored securely in between elections, and if it's not, it would be much easier for an attacker to have that kind of physical access to tamper with the programming inside the machine," Halderman says. "Of course, we didn't. But if the students I brought over with me and I were criminal attackers, we could have reprogrammed those machines so that they would cheat in subsequent races. It would be very, very difficult for election officials to tell that that had happened."

Nobody from Superior Township returned calls for comment.

The incident also reflects why Halderman isn't entirely at ease with Michigan's voting. The state's elections system is so decentralized that the front-line defense of democracy is left to township employees who often lack the imagination to understand how a lackadaisical approach in their office could undermine the confidence of an entire nation. There is often a "big disconnect between election officials' realization that elections face cybersecurity risks and their own assessments of their own local jurisdictions' security," Halderman says.

Halderman is pleased that election security is finally being taken more seriously, although he and others are troubled by President Trump's repeated and false claims that mail-in ballots "are very dangerous for this country because of cheaters." While Halderman notes that "a large fraction of all documented cases of electoral fraud that are prosecuted in the United States have to do with absentee ballots," he says that's because those attacks are exceptionally easy to detect and foil.

Rollow agrees: "It's not just a matter of you have to have access to somebody's mail and all of that, but you have to have access to their signature; you have to be able to copy it correctly. The risk that somebody would be taking to do this and the difficulty that they would have to entertain to do it at any scale to make any difference in a large election, it doesn't really pan out. That's why it's so infrequently attempted."

The bigger vote-by-mail problem, Halderman and Byrum agree, is that elections officials may not be prepared to handle the massive surge in absentee ballots expected this year. Byrum and others have been calling on the Michigan Legislature to allow county clerks to process ballots — that is, take them out of their envelopes, match the signatures, and prep them for the tabulators — before Election Day.

"If the Legislature doesn't act, it's going to be perhaps not a late night but a late morning after and perhaps a late afternoon after," Byrum says. "Seeds of doubt can easily be sown the longer it takes

Close

Tickets on Sale Now!

Get yours before they're gone!